Dr.WEB®

Antivirus
für Mac OS X *Light*

Defend what you create

Benutzerhandbuch

© 2009-2012 Doctor Web. Alle Rechte vorbehalten

Das im vorliegenden Dokument enthaltene Material ist Eigentum von Doctor Web und dient ausschließlich der persönlichen Nutzung durch Produktkäufer. Kein Teil des vorliegenden Dokumentes dard ohne Quellenangabe weder reproduziert noch auf einer Netzwerkressource untergebracht oder mittels Kommunikationskanäle und Massenmedien verbreitet oder auf jede andere Weise benutzt werden, ausgenommen Nutzung für persönliche Zwecke.

WARENZEICHEN
Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, Dr.Web AV-Desk und Dr.WEB Logo sind eingetragene Warenzeichen von Doctor Web in Russland und/oder anderen Ländern. Alle sonstigen eingetragenen Warenzeichen, Logos und Firmennamen, die im vorliegenden Dokument erwähnt sind, sind Eigentum ihrer jeweiligen Inhaber.

HAFTUNGSAUSSCHLUSS
Unter keinen Umständen haften Doctor Web und seine Lieferanten für die im vorliegenden Dokument enthaltenen Fehler und/oder Auslassungen sowie für Schäden des Produktkäufers (direkte oder indirekte Schäden einschließlich Gewinnausfälle), die sich dadurch ergeben.

Dr.Web® Light
Version 6.0.5
Benutzerhandbuch
13.02.2012

Doctor Web, Hauptsitz Russland
Tretja ul. Jamskogo polja 2, Gebäude 12A
125124 Moskau
Russische Föderation

Website: www.drweb.com
Telefon: +7 (495) 789-45-87

Nähere Informationen zu den regionalen Vertretungen und Büros finden Sie auf unserer Website.

Doctor Web

Doctor Web ist ein russischer Anbieter hauseigener IT-Sicherheitslösungen.

Doctor Web bietet effektive Antivirus- und Antispam-Lösungen sowohl für staatliche Einrichtungen und große Unternehmen als auch für private Benutzer.

Die Antivirensoftware von Dr.Web wird seit 1992 entwickelt. Die Antivirus-Lösungen zeigen immer wieder hervorragende Leistungen bei Entdeckung von Malware und entsprechen den weltweiten Sicherheitsnormen.

Zertifikate und Auszeichnungen sowie umfangreiche Geographie der Benutzer zeugen vom besonderen Vertrauen der Kunden in unsere Produkte.

Wir danken den Benutzern für Unterstützung der Lösungen von Dr.Web-Familie!

Inhaltsverzeichnis

Symbole und Abkürzungen 5

Kapitel 1. Einführung 7

- Über Dr.Web Light 7
- Systemanforderungen 8
- Installation und Deinstallation von Dr.Web Light 9

Kapitel 2. Hauptfunktionen 10

- Antivirusprogramm starten und beenden 11
- Aktualisierung 12
- Virenprüfung des Dateisystems 13
- Hilfe 15

Kapitel 3. Erweiterte Funktionen 16

- Ergebnisse 16
- Quarantäne 18
- Allgemeine Einstellungen 21
- Automatische Aktionen konfigurieren 21
- Dateien von der Prüfung auslassen 22
- Einstellungen zurücksetzen 23

Anhang 24

- Anhang A. Arten von Computerbedrohungen 24
- Anhang B. Beseitigung von Computerbedrohungen 31
- Anhang C. Tastenkombinationen 34
- Anhang D. Technischer Support 35

Schlagwortregister 36

Symbole und Abkürzungen

In der Anleitung werden folgende Bezeichnungen verwendet:

Bezeichnung	Kommentar
Fette Schrift	Elemente einer grafischen Benutzeroberfläche und Beispiele für Eingaben, die man exakt durchführen muss, wie sie in der Anleitung stehen.
Grüner und fetter Duktus	Die Name des Produktes **Doctor Web** oder deren Komponenten.
Grüner und unterstrichener Duktus	Links zu Hilfs- und Webseiten.
`Monoschrift`	Beispiele des Codes für die Kommandozeileneingabe und die Informationen, die an den Benutzer von der Anwendung ausgegeben wird.
Kursiv	Fachausdrücke und alternativer Text (wird statt Informationen geholt, die der Benutzer eingeben muss). Im Falle der Beispiele für die Kommandozeileneingabe wird kursiv auf die Parameterwerte anzeigen.
TITELBUCHSTABEN	Die Namen der Tasten auf der Tastatur.
Plus-Zeichen ("-")	Zeigt auf Tastenkombinationen. Zum Beispiel, Eintrag ALT-F1 bezeichnet, dass Sie die Taste ALT halten und dabei die Taste F1 drücken.
Ausrufezeichen	Wichtiger Hinweis oder eine Warnung vor potenziell gefährlichen oder folgenschweren Situationen.

In der Anleitung werden folgende Abkürzungen verwendet:

- OS – Betriebsystem
- CPU – Central Processing Unit
- GUI – Graphical User Interface (grafische Benutzeroberfläche)
- RAM – Random Access Memory (Hauptspeicher)

Kapitel 1. Einführung

Wir bedanken uns bei Ihnen, dass Sie sich für **Dr.Web® Light** entschieden haben. Diese Anwendung bietet einen sicheren Schutz gegen verschiedene Arten von Computerbedrohungen, verwendet dabei modernste Technologie zur Erkennung und Neutralisierung von Viren.

Dieses Handbuch soll den Benutzern von Computern unter Mac OS X bei der Installation und Verwendung von **Dr.Web Light** helfen.

Über Dr.Web Light

Dr.Web Light ist für Benutzer von Computern unter Mac OS bestimmt, die ihre Rechner Arbeitsrechner vor Viren und sonstigen Typen von Bedrohungen schützen wollen.

Die Grundkomponente des Programms (*Antiviren-Engine* und *Virendatenbanken*) ist effektiv und hat geringe Systemranforderungen. Zu den Vorteilen gehört auch die Plattfiormunabhängigkeit des Produktes. Die Komponenten von **Dr.Web Light** werden ständig aktualisiert. Dies sorgt für einen Virenschutz auf dem höchsten Niveau bietet. Für den Schutz von unbekannten Viren wird die Heuristische Analyse verwendet.

Dr.Web Light besteht aus folgenden Komponenten:

Komponente	Funktionen
Scanner	Dies ist eine Grundkomponente für die Erkennung von Viren, die ausführen kann: • Schnelles, vollständiges oder ein stichprobeartiges System-Scannen nach Anfrage des Benutzers • Neutralisierung von erkannten Bedrohungen (Behandlung, Entfernung, Verschiebung in Quarantäne; der Benutzer kann manuell gewünschte Aktion wählen, oder eine automatische Aktionsanwendung, angegeben für die Art der Bedrohung in der Antivirus-Einstellungen eingeben)
Quarantäne	Dies ist ein spezieller Ordner, der für die Isolierung von infizierten Dateien und andere Bedrohungen verwendet wird, damit sie dem System nicht schaden könnten.
Updater	Diese Komponente wird zu den Updates der Virendatenbanken und andere Komponente des Antivirus durch das Internet benutzt.

Flexible und bequeme Einstellungen von **Dr.Web Light** erlauben es Ihnen, Audio-Mitteilungen für verschiedene Ereignisse einzustellen, Aktionen für entdeckte Bedrohungen sowie Zeitabstände für Aktualisierung von Virendatenbanken zu konfigurieren, die Liste von Dateien und Verzeichnissen zu erstellen, die von der Prüfung ausgenommen werden sollen.

Systemanforderungen

Dr.Web Light ist für Computer unter Mac OS X 10.6.6 oder höher geeignet. Weitere Konfigurationsanforderungen entsprechen den Konfigurationsanforderungen jeweiliger Betriebssysteme.

Installation und Deinstallation von Dr.Web Light

Dr.Web Light Antivirus wird als ein mountbares Image (**drweb-light-605-macosx.dmg**) geliefert. Sie können diese Datei unter www.freedrweb.com herunterladen.

Anwendung installieren

1. Gegebenenfalls doppelklicken Sie auf die Image-Datei **drweb-light-605-macosx.dmg**, um das Image zu aktivieren.
2. Ziehen Sie die Datei der Anwendung vom Disk-Image in den Programme-Ordner auf Ihrem Mac.

Anwendung deinstallieren

Um **Dr.Web Light** zu deinstallieren, genügt es, die Anwendung in den Papierkorb zu verschieben. Gegebenenfalls geben Sie den Namen und das Passwort des Administrator-Kontos im entsprechenden Dialogfenster ein.

Antivirus aktualisieren

Je nach Erscheinen neuer Versionen von **Dr.Web Light** Antivirus werden die Updates unter www.freedrweb.com verfügbar gemacht.

Um ein Update für **Dr.Web Light** zu installieren, gehen Sie wie folgt vor:

1. Laden Sie das Disk-Image der neuen Antivirus-Version von der Website www.freedrweb.com herunter.
2. Führen Sie die oben im Bereich Anwendung installieren beschriebenen Aktionen aus.

Kapitel 2. Hauptfunktionen

Dieses Kapitel enthält Informationen darüber, wie man **Dr.Web Light** startet, beendet und aktualisiert. Dabei erhalten Sie einen Überblick über die Prüfung des Systems und die Hilfe, die Sie anfordern können.

Der Zugriff auf grundlegende Funktionen von **Dr.Web Light** wird aus dem Hauptfenster des Programms ausgeführt (s. Abbildung unten), dass aus den folgenden Abschnitten besteht und zur Steuerung und den Zugriff auf Antiviruskomponenten verwendet wird:

Abschnitt	Beschreibung
Schalter	In diesem Abschnitt können Sie: • Information zu der zuletzt ausgeführten Prüfung des Systems einsehen und schnelle bzw. vollständige Prüfung des Systems sowie benutzerdefinierte Prüfung einzelner Dateien und Ordner starten • sich über die letzten Updates informieren und bei Bedarf das Update manuell starten (siehe Aktualisierung) • auf die Abschnitte **Bedrohungen** und **Mein Dr.Web** umschalten
Bedrohungen	In diesem Abschnitt können Sie die Liste der bei der Prüfung entdeckten Bedrohungen einsehen, Aktionen zu deren Neutralisierung ausführen sowie zur Ansicht und Verwaltung des **Quarantäne**-Inhalts wechseln.
Mein Dr.Web	In diesem Abschnitt können Sie die Lizenz für erweiterte Version von **Dr.Web Light** bestellen sowie Neuigkeiten von Doctor Web, laufende Aktionen und aktuelle Informationen zu Viren einsehen.

Abbildung 1. Hauptfenster des Programms.

Des Weiteren können Sie aus dem Hauptfenster von **Dr.Web Light** zu Seiten von **Doctor Web** in sozialen Netzwerken Twitter und Facebook sowie auf YouTube wechseln.

Antivirusprogramm starten und beenden

Antivirusprogramm starten

Um **Dr.Web Light** zu starten, führen Sie eine der folgenden Aktionen durch:

- Öffnen Sie im Finder das Verzeichnis **Programme** und starten Sie **Dr.Web Light**.
- Rufen Sie Launchpad auf und starten Sie **Dr.Web Light**.

Beim Programmstart werden die Aktualisierungeinstellungen überprüft. Gegebenenfalls werden die Updates für das Programm heruntergeladen.

Beim ersten Start des Programms wird die Aktualisierung gestartet, einschließlich Herunterladen von Virendatenbanken. Dieser Vorgang kann längere Zeit in Anspruch nehmen.

Antivirusprogramm beenden

Um **Dr.Web Light** zu beenden, führen Sie eine der folgenden Aktionen durch:

- Wählen Sie **Dr.Web® für Mac OS X beenden** in Programmmenü (Menüleiste am oberen Rand des Desktops) aus.
- klicken Sie auf das Anwendungssysmbol in Dock und halten Sie die linke Maustaste gedrückt, danach wählen Sie im Menü **Beenden** aus.
- Drücken Sie die Tastenkombination COMMAND-Q.

Aktualisierung

Auf der ganzen Welt tauchen immer wieder neue Typen von Computerbedrohungen mit verbesserten Tarntechniken auf. Die Aktualisierung von Virendatenbanken sowie anderen Komponenten von **Dr.Web Light** gewährleistet, dass Ihr Rechner auf dem neuesten Sicherheitsstand gehalten und vor neuen Bedrohungen geschützt wird. Die Aktualisierung wird durch den **Updater** durchgeführt.

Beim ersten Starten von **Dr.Web Light** ist es erforderlich, vor Arbeitsbeginn die Virendatenbanken auf den aktuellen Stand zu bringen. Weitere Aktualisierung wird mit den Zeitabständen, die Sie in den Einstellungen von **Dr.Web Light** konfigurieren können, erfolgen.

Zeitabstände für Aktualisierung von Virendatenbanken konfigurieren

1. Im Anwendungsmenü klicken Sie auf **Einstellungen** und wechseln Sie auf die Registerkarte **Update**.
2. Gegebenenfalls ändern Sie die Zeitabstände für Herunterladen von Updates.

Virenprüfung des Dateisystems

Dr.Web Light Antivirus führt eine Überprüfung der Dateisystem-Objekte auf Anforderung des Benutzers aus. Dabei werden die Bedrohungen, die ihre Anwesenheit im System verschleiern, entdeckt. Zum sicheren Schutz des Computers ist es erforderlich, die Systemprüfung mit Hilfe von **Dr.Web Light** von Zeit zu Zeit zu starten.

Beim Scannen steigt die Prozessorbelastung. Dies kann schnelle Batterie-Entleerung zur Folge haben. Es ist empfehlenswert, Laptops nur im Netzbetrieb zu prüfen.

Systemprüfung starten

1. Im Hauptfenster von **Dr.Web Light** Wählen einen bestimmten Scanmodus aus:
   - **Schnell** – in diesem Modus werden besonders anfällige Orte des Systems überprüft.
   - **Vollständig** – in diesem Modus wird das gesamte Dateisystem überprüft.

   Sie können auch spezielle Tastenkombinationen CONTROL-COMMAND-E und CONTROL-COMMAND-F auf der Tastatur zum Starten der schnellen bzw. vollständigen Prüfung verwenden.

2. Um einzelne Dateien und Ordner zu prüfen, ziehen Sie die zu prüfenden Dateien und Ordner ins Hauptfenster des Antivirusprogramms bzw. klicken Sie auf den punktierten Bereich im linken Teil des Programmhauptfensters.

   In der geöffneten Objektliste geben Sie die zu prüfenden Dateien und Ordner an:

   - Um ein Objekt der Liste hinzuzufügen, klicken Sie auf unterhalb der Objektliste bzw. ziehen Sie dieses Objekt in die Liste.

- Um ein Objekt von der Liste zu streichen, heben Sie es hervor und klicken Sie auf , bzw. ziehen Sie es aus dem Programmfenster.

Klicken Sie auf den **Prüfen**-Button, um die Prüfung der ausgewählten Objekte zu starten.

Nach der Prüfung wird man über das Hauptfenster zur Registerkarte Ergebnisse gewechselt. Sie können die Prüfung anhalten bzw. stoppen, indem Sie die Verwaltungstasten **Pause** und **Stop** verwenden.

Die Dateien können auch beim Scannen übersprungen werden, wenn sie beschädigt oder passwortgeschützt. Um übersprungene Objekte zu prüfen, entpacken Sie die Archive vor Prüfung.

Dr.Web Light erfordert die Administratorrechte, um den Zugriff auf kritische Bereiche der Festplatte zur weiteren Überprüfung zu bekommen.

Administratorrechte konfigurieren

Dr.Web Light erfordert die Administratorrechte, um den Zugriff auf kritische Bereiche der Festplatte zur weiteren Überprüfung zu bekommen. Damit **Dr.Web Light** permanente Administratorrechte erhält, gehen Sie wie folgt vor:

- kKicken Sie auf im unteren Fensterbereich, wählen Sie die Option **Mit Administratorrechten arbeiten** und geben Sie das Administrator-Passwort ein.
- Auf der Tastatur drücken Sie die Tastenkombination COMMAND-SHIFT-A und geben Sie das Administrator-Passwort ein.
- Klicken Sie auf das Schloss-Symbol im unteren Fensterbereich und geben Sie das Administrator-Passwort ein.

Hilfe

Um die Hilfe zu erhalten, wählen Sie via Apple Help **Dr.Web Hilfe** aus, Zugang zu deren wird mit Hilfe des Viewers Apple Help ermöglicht.

Dr.Web Hilfe aufrufen

Um **Dr.Web Hilfe** aufzurufen, wählen Sie **Hilfe Dr.Web** oben auf dem Desktop in Menü **Hilfe** oder geben Sie ein Wort in das entsprechende Feld ein.

Wenn Sie nicht geschafft haben, das Problem zu lösen oder eine Antwort auf Ihre Frage zu Antivirus **Dr.Web Light** zu finden, wenden Sie sich an technischen Support.

Kapitel 3. Erweiterte Funktionen

In diesem Kapitel finden Sie Informationen zu den Antivirus-Funktionen sowie dazu, welche Einstellungen von **Dr.Web Light** geändert werden können.

Ergebnisse

Nach der Prüfung wird man über das Hauptfenster zur Registerkarte Ergebnisse gewechselt (s. Abbildung unten). Im Laufe der Prüfung werden folgende Informationen in diesem Fenster angezeigt:

- Startzeit der Prüfung
- Anzahl der geprüften Objekte
- Zeit bis zum Ende der Prüfung
- Anzahl der entdeckten Bedrohungen
- Name der Datei, die jetzt überprüft wird

Im unteren Fensterbereich können Sie die Statistik für die aktuelle Prüfung einsehen:

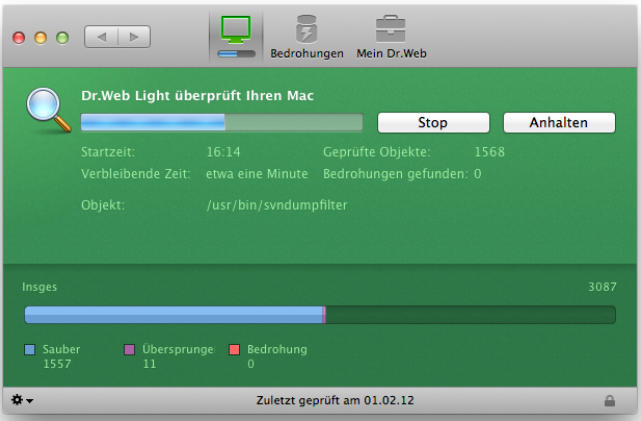

Abbildung 2. Anschauen der Scan-Ergebnisse.

Am Ende der Prüfung wird es Ihnen angeboten, die entdeckten Bedrohungen zu neutralisieren. Sie können automatische Aktionen des Antivirusprogramms für verschiedene Bedrohungstypen konfigurieren bzw. Aktionen für Bedrohungen manuell ausführen. Klicken Sie auf den **Neutralisieren**-Button, um die in den Antivirus-Einstellungen festgelegten Aktionen für alle entdeckten Bedrohungen zu verwenden. Sie können auch den Bereich mit Bedrohungen öffnen, um Aktionen für deren Neutralisierung manuell auszuwählen.

Informationen zu Bedrohungen einsehen

1. Um die Liste mit entdeckten Bedrohungen einzusehen, öffnen Sie den Bereich **Bedrohungen**. In der Statuszeile im unteren Fensterbereich wird die Gesamtzahl der entdeckten Bedrohungen und deren Gesamtgröße sowie die Anzahl und Größe der markierten Objekte angezeigt.

2. Um Informationen zu Bedrohung einzusehen:
   - Klicken Sie auf den Pfeil rechts neben dem Namen der Datei, die diese Bedrohung beinhaltet.
   - Klicken Sie auf bzw. drücken Sie die Tastenkombination COMMAND-SHIFT-S auf der Tastatur, um die Seitenleiste mit folgenden Informationen zu Bedrohung zu öffnen: Name der Bedrohung, Name der Datei, die diese Bedrohung beinhaltet, Dateityp, Dateigröße, Erstellungsdatum sowie Datum der Dateimodifikation. Um weitere Informationen zu Bedrohung einzusehen, klicken Sie auf den **Detailliert**-Button.
3. Um sich mit Informationen zum ähnlichen Bedrohungstyp auf der Website von **Doctor Web** vertraut zu machen, klicken Sie auf den Bedrohungsnamen im Fenster mit detaillierten Informationen dazu.

Schädliche Objekte bearbeiten

1. Öffnen Sie den Bereich **Bedrohungen**.
2. Um die in den Antivirus-Einstellungen für bestimmten Bedrohungstyp festgelegte Aktion auszuführen, klicken Sie auf den Button mit dieser Aktion, die sich unter Bedrohungsnamen befindet, bzw. auf den Pfeil an diesem Button, um erforderliche Aktion auszuwählen.
3. Um eine Aktion für mehrere Bedrohungen auszuführen, markieren Sie diese (dafür halten Sie die SHIFT-Taste gedrückt), klicken Sie auf und wählen Sie die Aktion in der Liste aus.

Sie können auch spezielle Tastenkombinationen auf der Tastatur verwenden.

Quarantäne

Die **Quarantäne** ist ein Spezialordner, der zur Isolation gefundener Bedrohungen dient. Die Isolation ist notwendig, wenn das verschobene Objekt nützlich ist, im Moment aber nicht desinfiziert werden kann.

Isolierte Objekte können möglicherweise nach nächsten Update des Programms desinfiziert werden.

Aus Vertraulichkeitsgründen wird ein separater **Quarantäne**-Ordner für jeden Benutzer erstellt. Wenn Sie mit Administratorrechten arbeiten, werden die entdeckten Bedrohungen in **Quarantäne** des Administrators verschoben und in **Quarantäne** der Benutzer nicht zugänglich sein.

Auf der Registerkarte **Quarantäne** des Bereiches **Bedrohungen** können Sie den **Quarantäne**-Inhalt über die Benutzeroberfläche von **Dr.Web Light** (s. Abbildung unten). In der Statuszeile im unteren Fensterbereich wird die Gesamtzahl von Bedrohungen und deren Gesamtgröße sowie die Anzahl und Größe der markierten Objekte angezeigt.

Informationen zu Bedrohungen einsehen

1. Führen Sie eine von folgenden Aktionen durch:
   - Klicken Sie auf den Pfeil rechts neben dem Namen der Datei, die diese Bedrohung beinhaltet.
   - Klicken Sie auf bzw. drücken Sie die Tastenkombination COMMAND-SHIFT-S auf der Tastatur, um die Seitenleiste mit folgenden Informationen zu Bedrohung zu öffnen: Name der Bedrohung, Name der Datei, die diese Bedrohung beinhaltet, Dateityp, Dateigröße, Erstellungsdatum sowie Datum der Dateimodifikation. Um weitere Informationen zu Bedrohung einzusehen, klicken Sie auf den **Detailliert**-Button.
2. Um sich mit Informationen zum ähnlichen Bedrohungstyp auf der Website von **Doctor Web** vertraut zu machen, klicken Sie auf den Bedrohungsnamen im Fenster mit detaillierten Informationen dazu.

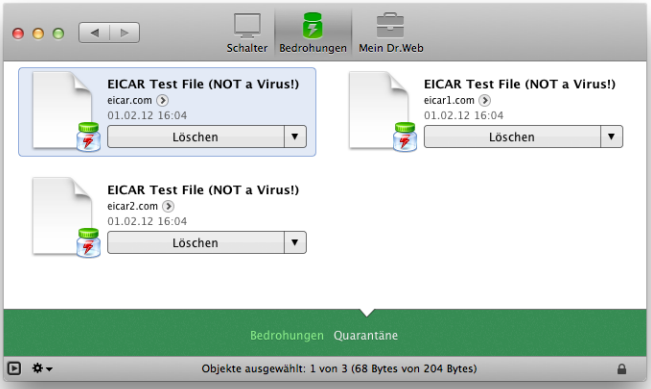

Abbildung 3. Liste der Objekte, die in Quarantäne verschoben wurden.

Objekte in Quarantäne bearbeiten

1. Um empfohlene Aktion für Objekt in der **Quarantäne** auszuführen, klicken Sie auf den Button mit dieser Aktion, die sich unter dem Objekt befindet, bzw. auf den Pfeil an diesem Button, um erforderliche Aktion auszuwählen. Sie können eine der folgenden Aktionen auswählen:
   - **Löschen** – die Datei vom Dateisystem unwiderruflich löschen.
   - **Desinfizieren** – versuchen, die Datei zu desinfizieren.
   - **Wiederherstellen** – die Datei aus der **Quarantäne** an den ursprünglichen Ort zurück verschieben.
   - **Wiederherstellen als** – Pfad für Wiederherstellung der Datei aus der **Quarantäne** angeben.
2. Um eine Aktion für mehrere Objekte gleichzeitig auszuführen, markieren Sie diese (dafür halten Sie die SHIFT-Taste gedrückt), klicken Sie auf und wählen Sie die Aktion in der Liste aus.

Sie können auch spezielle Tastenkombinationen auf der Tastatur verwenden.

Allgemeine Einstellungen

Sie können akustische Benachrichtigungen für verschiedene Ereignisse, Arbeit im Administratormodus sowie die Prüfung beim Akkubetrieb konfigurieren.

Allgemeine Einstellungen

1. Im Anwendungsmenü klicken Sie auf **Einstellungen** und wechseln Sie auf die Registerkarte **Basis**.
2. Gegebenenfalls können Sie die Einstellungen ändern:
   - Aktivieren Sie die Verwendung von akustischen Benachrichtigungen.
   - Wechseln Sie in den Administratormodus. Die Arbeit mit Administratorrechten ermöglicht, dass die bei der Prüfung im Benutzermodus übersprungenen Objekte gescannt werden.
   - Aktivieren Sie die Anforderung zur Fortsetzung der Prüfung im Akkubetrieb.

Automatische Aktionen konfigurieren

Sie können Aktionen konfigurieren, die zu diversen Typen von Computerbedrohungen vorgenommen werden sollen, wenn eine Aktion manuell nicht durchgeführt werden soll.

Automatische Antivirus-Reaktion einstellen

1. Klicken Sie im Hauptmenü auf **Einstellungen** und öffnen Sie den Tab **Aktionen**.
2. Ändern Sie bei Bedarf automatische Aktionen für entsprechende Typen der Bedrohungen.
3. Damit die Aktionen automatisch ausgeführt werden, setzen Sie ein Häkchen bei **Aktionen automatisch ausführen**.

Dabei werden auch die Aktionen, die auf den Buttons unterhalb der **Bedrohungen** im Bereich Einstellungen angegeben sind, gemäß den festgelegten Einstellungen geändert.

Es wird nicht empfohlen, die Default-Einstellungen zu ändern, wenn es nicht notwendig ist.

Dateien von der Prüfung auslassen

Bei Bedarf kann eine Liste von Dateien bzw. Verzeichnissen erstellt werden, die von der Prüfung ausgenommen werden sollen.

Ausnahmeliste konfigurieren

1. Um die Liste der Ausnahmen, die durch **Dr.Web Light**, im Anwendungsmenü klicken Sie auf **Einstellungen** und wechseln Sie auf die Registerkarte **Ausnahmen**.
2. Gegebenenfalls können Sie die Einstellungen ändern:
   - Um ein Objekt der Ausnahmeliste hinzuzufügen, klicken Sie auf und geben Sie das erforderliche Objekt an bzw. ziehen Sie es in die Liste.
   - Um Objekte von der Ausnahmeliste zu löschen, markieren Sie diese in der Liste und klicken Sie auf bzw. ziehen Sie diese Objekte aus dem Programmfenster.
   - Um die Ausnahme des Objektes von der Prüfung vorübergehend rückgängig zu machen, ohne dabei das Objekt von der Liste zu streichen, reicht es aus, das Häkchen bei **Ausnehmen** rechts von diesem Objekt abzuwählen.
   - Um Archive vor deren Prüfung zu entpacken, setzen Sie ein Häkchen bei **Inhalt der Archive prüfen**.

Es wird nicht empfohlen, die Default-Einstellugen der Ausnahmelisten ohne Bedarf zu ändern.

Einstellungen zurücksetzen

Gegebenenfalls können Sie alle benutzerdefinierten Einstellungen des Antivirusprogramms zurücksetzen und die Default-Parameter der Anwendung wiederherstellen:

1. Im Anwendungsmenü klicken Sie auf **Einstellungen** und wechseln Sie auf die Registerkarte **Zurücksetzen**.
2. Klicken Sie auf **Default-Parameter wiederherstellen**.
3. Bestätigen Sie die Zurücksetzung von benutzerdefinierten Einstellungen und die Wiederherstellung der ursprünglichen Parameter von **Dr.Web Light**.

Anhang

Anhang A. Arten von Computerbedrohungen

Unter dem Begriff *Bedrohung* versteht man im diesem Kontext beliebiges Programm, das direkt oder indirekt Ihre Rechner, Netzwerk oder Benutzerrechte beschädigen kann (d.h. schädliche und andere ungewünschte Programme). In weiterem Sinne des Begriffs bedeutet es, beliebige potentielle Gefahr für Rechner oder Netzwerk (d.h. Gefahr der Anfälligkeit und Möglichkeit des Hacker-Angriffs).

Alle unten beschriebenen Programmtypen sind für Benutzerdaten oder vertrauliche Benutzerrechte potentiell gefährlich. Programme, die nicht geheim im System laufen (z.B. einige Spam-Verteilerprogramme oder Traffic-Analyse Tools), werden normalerweise nicht als Computerbedrohungen bezeichnet, obwohl sie dem Benutzer unter bestimmten Umständen Schaden zufügen können.

In Produkten und Unterlagen von **Doctor Web** werden Bedrohungen konventionell in zwei Arten nach Gefährlichkeit geteilt:

- **Wesentliche Bedrohungen** sind die klassischen Bedrohungen für Rechner, die von selbst diverse zerstöririschen und illegalen Aktionen im System verursachen können (z.B. Löschen und Entwenden von wichtigen Informationen, Netzwerkabsturz usw.). Diese Art von Computerbedrohung umfasst Software und Programme, die konventionell als Malware bezeichnet werden (Viren, Würmer und Trojaner).

- **Unwesentliche Bedrohungen** sind auch Computerbedrohungen, die als weniger gefährlich im Vergleich zu wesentlichen Bedrohungen gelten, aber müssen auch möglichst vermieden werden, denn sie können von Drittpersonen zugegriffen werden, um schädliche Aktionen zu verursachen. Darüber hinaus ist die Existenz von unwesentlichen Bedrohungen im System ein offensichtliches Zeichen von einem niedrigen Sicherheitsniveau des Systems. In der Informatikfachsprache wird dieser Typ von Computerbedrohungen als Grayware oder PUP (potentially unwanted programs) bezeichnet. Dazu gehören solche Programme, wie Adware, Einwahlprogramme (Dialer), Scherzprogramme, potentiell gefährliche Programme und Hacktools.

Wesentliche Bedrohungen

Computerviren

Dieser Typ von Computerbedrohungen zeichnet sich durch die Fähigkeit aus, seinen Code in den ausgeführten Code von anderen Programmen einzubringen. Dieses Eindringen wird als *Infizierung* bezeichnet. In den meisten Fällen wird die infizierte Datei zum Virenträger, und der eingebrachte Code entspricht nicht unbedingt völlig dem Originalcode. Der grösste Teil des Virus wird zur Beschädigung oder Vernichtung von Daten generiert.

Bei **Doctor Web** werden Viren nach Dateityp klassifiziert:

- **Dateiviren** infizieren Daten des Betriebsystems (normalerweise ausführbare Dateien und dynamische Bibliotheken) und werden beim Zugriff auf die infizierte Datei aktiviert.
- **Makroviren** infizieren Dokumente, die von Microsoft® Office Anwendungen benutzt werden (und andere Programme, die Makros benutzen, die z.B. in Visual Basic geschrieben sind). Makros sind eingebaute Programme, die in einer vollständigen Programmiersprache geschrieben sind, und können unter bestimmten Bedingungen gestartet werden (z.B. in Microsoft® Word können Makros beim Öffnen/Schließen/Speichern der Datei gestartet werden).

- **Skriptviren** werden in Skriptsprachen geschrieben und infizieren in den meisten Fällen andere Skriptdateien (z.B. Betriebssystemdateien). Sie können auch andere Dateitypen infizieren, die das Ausführen der Scripts unterstützen. So werden besonders anfällige Scripts in Webanwendungen infiziert.
- **Bootviren** infizieren den Bootsektor von Disketten und Festplattenpartitionen, und auch den Master Boot Record (MBR) einer Festplatte. Sie benötigen ganz wenig Speicherplatz und bleiben bereit, ihre Funktionen zu realisieren, solange das System nicht heruntergefahren, neu gestartet oder beendet wird.

Die meisten Viren verfügen über bestimmte Abwehrmechanismen gegen die Entdeckung. Abwehrverfahren gegen die Entdeckung werden ständig verbessert, und dabei werden immer neue Mechanismen zur Überwindung dieser Abwehr entwickelt. Viren können auch nach Abwehrprinzip gegen die Entdeckung klassifiziert werden:

- **Verschlüsselte Viren** verschlüsseln ihren Code bei jeder neuen Infizierung, um die Entdeckung in einer Datei, im Speicher oder im Bootsektor zu komplizieren. Jedes Exemplar vom solchen Virus enthält nur ein kurzes gemeinsames Fragment (Entschlüsselungsverfahren), das als eine Signatur ausgewählt werden kann.
- **Polymorphe Viren** benutzen neben der Codeverschlüsselung ein Spezialentschlüsselungsverfahren, das sich selbst bei jedem neuen Virus verändert. Dies führt dazu, dass das Virus keine Bytesignaturen enthält.
- **Stealth-Viren** (Tarnviren) führen spezielle Aktionen zur Tarnung ihrer Aktivitäten durch, mit dem Ziel ihre Existenz in den infizierten Objekten zu verschleiern. Computerviren dieser Art nimmt vor der Infektion die Programmparameter der Datei auf, und danach gibt der Datei die Daten der ursprünglichen Datei zurück.

Viren können auch nach Sprache klassifiziert werden, in der sie geschrieben sind (Mehrheit wird in Assemblersprache, Hochsprachen, Skriptsprachen etc. geschrieben) und auch nach Betriebssystemen.

Würmer

In letzter Zeit kommen Würmer immer häufiger als Viren und andere Malware vor. Genauso wie die Viren, können solche Programme Ihre Kopien vervielfältigen, aber sind unfähig, andere Computerprogramme zu infizieren. Ein Wurm dringt in den Rechner aus dem Netzwerk ein (meistens als Anhang in einer E-Mail oder über das Internet) und verschickt seine Funktionskopien an andere Computernetzwerke. Dabei um die Verbreitung zu starten, können Würmer sowohl Benutzerdaktionen als auch ein automatisches Verfahren zum Auswahlen und Angreifen des Rechners benutzt.

Würmer bestehen nicht unbedingt nur aus einer Datei. Bei vielen Würmern gibt es einen so genannten Infizierungsteil (Shellcode), die in den Arbeitsspeicher geladen wird und lädt unmittelbar den Körper als ausfuhrbare Datei zu. Solange der Wurmkörper ins System nicht eingedrungen ist, kann dem Würmer durch Neustart vom Rechner (dabei soll Arbeitsspeicher reseten) loswerden. Wenn der Würmerkörper sich im System finden soll, dann hilft nur ein Antivirus-Programm.

Aufgrund der intensiven Verbreitung können Würmer Netzwerkeabstürze verursachen, sogar wenn sie indirekt das System beschädigen.

Bei **Doctor Web** werden Würmer nach Verbreitungsstrategie klassifiziert:

- **Netzwurm** verbreitet sich mit Hilfe von diversen Netzwerk- und Transferprotokollen.
- **E-Mail-Wurm** verbreitet sich mit Hilfe von Protokollen (POP3, SMTP etc.).
- **Instant-Messaging-Wurm** verbreitet sich über populäre Instant-Messaging-Software (ICQ, IM, IRC etc.).

Trojanische Pferde (Trojaner)

Malware dieser Art ist unfähig, sich selbst zu vervielfältigen. Trojaner ersetzen eine oft ausführbare Anwendung und führen aus oder imitieren Ihre Funktionalität, aber gleichzeitig erfüllen im Hintergrund

eine andere schädliche Funktion (Verletzung oder Löschen von Daten, Übertragung vertraulicher Angaben etc.), oder ermöglicht einen unbefugten Zugriff zum Rechner von einer fremden Person, z.B. um einer Drittperson einen Schaden zuzufügen.

Ein Trojaner verfügt über die virenähnlichen Tarn- und Schadfunktionen und kann sich sogar als ein Virenmodul erweisen. Aber hauptsächlich verbreiten sich Trojaner als einzelne ausführbare Dateien (legen sich auf Tauschbörsen ab, speichern sich auf Dateiträgern oder werden über E-Mails versandt), die entweder vom Anwender, oder von einem Systemprozess ausgeführt werden.

Es ist sehr schwierig, Trojanerprogramme zu klassifizieren. Erstens, weil sie sich oft mit Viren und Würmern verbreiten. Zweitens, werden schädliche Aktionen normalerweise zur Kategorie Trojaner zugerechnet, sogar wenn sie durch andere Arten von Bedrohungen verursacht werden können. Unten sind einige Typen von Trojanerprogrammen aufgelistet, die bei **Doctor Web** klassifiziert werden:

- **Backdoors** bezeichnen einen Trojaner, der unter Umgehung der normalen Zugriffssicherung Zugang zum Computer ermöglicht. Backdoors infizieren nicht die Dateien, sondern schreiben sich im Verzeichnis, dabei werden Schlüsseln modiifiziert.
- **Rootkits** ist eine Sammlung von Softwarewerkzeugen, die nach dem Einbruch in ein Betriebssystem installiert werden, um sich selbst im System zu tarnen. Zudem kann ein Rootkit Prozesse anderer Programme, Logins, Ordner, Dateien verstecken. Rootkit verbreitet sich als ein selbständiges Programm oder als eine Zusatzkomponente als Bestandteil eines Schadprogramms. Rootkits werden bedingt nach Schadroutine in zwei Gruppen geteilt: User Mode Rootkits (UMR) – läuft im Usermodus (Einbruch in Bibliotheksfunktionen des Usermodus) und Kernel Mode Rootkits (KMR) – läuft im Kernelmodus (Einbruch in Funktionen auf der Kernelebene, was wesentlich Entdeckung und Neutralisierung kompliziert).
- **Tasten-Recorder** (Keyloggers) wird dazu verwendet, um die Eingaben eines Benutzers mitzuprotokollieren. Dabei wird das Ziel verfolgt, vertrauliche Daten zu entwenden (z.B. Schlüsselwörter, Logins, Kreditkartennummer etc.).

- **Trojan-Clicker** – hier werden Links beim Klicken umgeleitet. Normalerweise wird Benutzer auf bestimmte Adressen umgeleitet, um Internet-Traffic mit Werbeihalt zu erhöhen. Damit können auch DDoS-Angriffe unternommen werden.
- **Trojan-Proxy** ermöglicht einem Verbrecher den stillen Zugrang ins Internet über den Opferrechner.

Außer oben genannten können Trojaner auch andere Schadaktionen durchführen, z.B. Startseite in Ihrem Browser ändern oder bestimmte Daten löschen. Jedoch können solche Aktionen auch von anderen Bedrohungen durchgeführt werden (z.B. von Viren und Würmern).

Unwesentliche Bedrohungen

Hackertools

Hackertools sollen zur Unterstützung eines Hackers dienen. Meistverbreitet sind Portscanner, änfallige Stellen von Firewall und anderen Sicherheitskomponenten überprüfen. Außer Hacker können solche Tools von Systemadministratoren benutzt werden, um Sicherheit Ihrer Netzwerke zu überprüfen. Manchmal werder zu Hackertools solche Programme zugerechnet, die Sozial Engineering verwenden.

Adware

Am häufigsten bezeichnet man mit diesem Begriff einen Programmcode, der in einer kostenlosen Software eingebaut ist und sorgt dafür, dass dem Benutzer Werbungen gezeigt wird. Jedoch kann solcher Code sich geheim mit Hilfe von anderen Schadprogrammen verbreiten, und z.B. in Internetbrowser Werbung anzeigen. Oft nutzt Adware die von Spyware gesammelten Daten.

Scherzprogramme

Die Art von Malware, die genauso wie Adware für das System nicht direkt schädlich ist. Meist generiert das Programm Benachrichtigungen über nicht-existierende Fehler und droht mit entsprechenden Aktionen, die angeblich zur Datenbeschädigung führen kann. Die Scherzprogramme sollen lediglich jemanden erschrecken oder

zudringlich reizen.

Einwahlprogramme (Dialer)

Dialer sind spezielle Computerprogramme, die einen Telefonnummerbereich scannen und versuchen über das analoge Telefon eine kostenverursachende, oft horrend überteuer Wählverbindung zum Internet oder Computernetzwerken aufzubauen. Diese Programme gewährleisten den Verbindungsaufbau über eine entsprechende Premium-Rate-Nummer, dabei entstehen hohe Kosten für den Anwender.

Riskware

Normale Computerprogramme, die nicht als Schadprogramme entwickelt sind, aber können trotzdem die Systemsicherheit bedrohen. Dabei sind das nicht nur Programme, die zufällig Daten beschädigen oder löschen können, aber auch welche, die von Hackern oder anderen Programmen zur Systembeschädigung benutzt werden können. Dazu zählen diverse Offline-Kommunikationsprogramme, Verwaltungsprogramme, FTP-Server usw.

Verdächtige Objekte

Dazu zählen alle potentielle Bedrohungen, die mit der heuristischen Analyse endteckt wurden. Solche Objekte können Computerbedrohungen beliebiger Art sein (vielleicht sogar unbekannte für IT-Sicherheitsspezialisten). Wegen einer Fehldiagnose können sich solche Objekte aber als ungefährliche erweisen. Verdächtige Objekte sollen zur Analyse im **Virenlabor von Doctor Web** geschickt werden.

Anhang B. Beseitigung von Computerbedrohungen

Es gibt eine Menge an Verfahren zur Entdeckung und Neutralisierung der Computerbedrohungen. Viele von diesen Verfahren stehen Ihnen in den Produkten von **Dr.Web** zur Verfügung, um mit ihren flexiblen und benutzerfreundlichen Einstellungen ein hohes Sicherheitsniveau von Ihren Rechnern und Netzwerken zu gewährleisten.

Entdeckungsverfahren

Suche nach Kontrollsummen

Dieses Verfahren ist eine Art von Signaturanalyse. *Signatur* ist eine kontinuerliche endliche Byte-Reihnfolge, die einzigartig für eine bestimmte Computerbedrohung definiert ist. Falls beim Scannen des Codes der gescannten Programm eine Signatur aus der Virendatenbank getroffen wird, dann wird der Fund als Computerbedrohung registriert.

Unter Suche nach Kontrollsummen versteht man den Vergleich von Kontrollsummen, nicht von den Signaturen, was zu einer wesentlichen Verringerung der Virendatenbankgröße führt, wobei bleibt das Verfahren hinsichtlich der Zuverlässigkeit mit der konventionellen Signaturanalyse vergleichbar ist.

Emulation

Die Emulationsmethode zur Ausführung des Programmcodes wird zur Entdeckung von polymorphen und verschlüsselten Viren eingesetzt, wenn die Suche nach Kontrollsummen von Signaturen unmöglich oder wesentlich komplizierter ist als die Erstellung zuverlässiger Signaturen. Das Verfahren basiert sich auf Simulation der Ausführung des zu analysierenden Codesdurch den *Emulator* (Prozessormodell). Der Emulator operiert mit einem geschützten Speicherbereich (*Emulationsbuffer*). Dabei werden Anweisungen zur Ausführung dem zentralen Prozessor nicht übermittelt. Wenn der Code infiziert ist, wird der Virus-Körper durch die Emulation entschlüsselt. Danach kann er

leicht durch die Suche nach Kontrollsummen von Signaturen entdeckt werden.

Heuristische Analyse

Heuristische Analyse wird zur Entdeckung von neuen Bedrohungen, die für Virendatenbanken unbekannt sind. Das Prinzip der heuristischen Analyse basiert sich auf der Ermittlung von häufig vorkommenden Malware-Kennungen bei Objekten und Addition der Punktwerte. Die Wesentlichkeit einer Kennung hängt von ihrem *Gewicht* ab. Wenn diese Kennung auf einen Schadcode hinweist, ist die Zahl positiv. Wenn eine Kennung unwesentlich ist, sit die Zahl negativ. Erreichen oder überschreiten diese Punkte den Schwellwert, wird die Datei als verdächtig (oder potentiell gefährlich) markiert.

Wie jedem anderen Prüfungssystem kann der Heuristik Fehler erster Ordnung (Übersehen einer unbakannten Bedrohung) und zweiter Ordnung (Falschdetektion) unterlaufen.

Origins Tracing™

Origins Tracing ist ein spezieller Algorithmus zum Erkennen von Computerbedrohungen, der ausschließlich in **Dr.Web** Produkten eingesetzt wird. Ergänzend zu den konventionellen Scannverfahren der Signatur- und Heuristischen Analysen, erhöht dieser Algorithmus wesentlich die Entdeckungswahrscheinlichkeit von unbekannten Bedrohungen. Der Name der Bedrohung, die durch **Origins Tracing** entdeckt wurde, wird mit der Endung **.Origin** ergänzt.

Aktionen

In Produkten von **Dr.Web** hat man die Möglichkeit, diverse Aktionen zu entdeckten Objekten vorzunehmen, um die Computerbedrohungen zu neutralisieren. Der Benutzer kann Default-Einstellungen zu bestimmten Bedrohungsarten lassen, ändern und die notwendige Aktion für jedes einzelnes Objekt vornehmen. Unten finden sich die verfügbaren Aktionen:

- **Desinfizieren** ist eine Aktion, die nur zu wesentlichen Bedrohungen (Viren, Würmer und Trojaner) vorgenommen wird. Dabei wird entweder der schädliche Code aus der infizierten Datei entfernt, oder werden die Funktionskopien des Programms gelöscht. Außerdem wird es versucht, die Struktur und Funktionsfähigkeit der infizierten Objekten wiederherzustellen. Nicht alle infizierte Dateien können desinfiziert werden, aber Produkte von Dr.Web basieren sich auf effizienteren Desinfektion- und Wiederherstellungssalgorithmen für Dateien im Vergleich zu Produkten von anderen Antivirus-Hersteller.
- **Quarantäne** (Verschieben in die Quarantäne) – hier wird das gefundene Objekt in einen Spezialordner verschoben, der vom System isoliert ist. Diese Aktion kann durchgeführt werden, falls das Löschen unmöglich ist, und auch für verdächtige Objekte. Es wird empfohlen, solche Objekte an unser **Virenlabor Doctor Web** zur Analyse zu schicken.
- **Löschen** gilt als die effizienteste Neutralisierungsmethode für alle Computerbedrohungsarten. Durchführen von dieser Aktion bedeutet, dass das gefährliche Objekt (oder sein Inhalt) endgültig entfernt wird. Denken Sie daran, dass das Löschen manchmal zu Dateien vorgenommen werden kann, für welche die Aktion **Desinfizieren** gewählt wurde. Solches "Desinfizieren durch Löschen" wird durchgeführt, wenn die Datei völlig aus dem schädlichen Code besteht und enthält keine nützliche Information mehr (z.B. unter Desinfizieren von einem Würmer versteht man das Löschen aller seinen Funktionskopien).
- **Ignorieren** (Überspringen) ist eine Aktion, die nur für unwesentliche Bedrohungen (Adware, Dialer, Scherzprogramme, Riskware und Hackertools) verwendet wird. Dabei werden weder Aktionen für Beseitigung der entdeckten Bedrohung noch Benachrichtigung des Benutzers ausgeführt.

Anhang C. Tastenkombinationen

Um die Prüfung zu starten, Aktionen für entdeckte Bedrohungen auszuführen sowie die Funktion von **Dr.Web Light** zu konfigurieren, können Sie spezielle Tastenkombinationen nutzen.

Tastenkombination		Beschreibung
Scanner-Menü	CONTROL-COMMAND-E	Schnelles Scannen
	CONTROL-COMMAND-F	Vollständiges Scannen
	CONTROL-COMMAND-C	Scan-Objekte auswählen
Aktionen-Menü	COMMAND-SHIFT-C	Desinfizieren
	COMMAND-SHIFT-M	In Quarantäne verschieben
	COMMAND-SHIFT-I	Ignorieren
	COMMAND-SHIFT-D	Löschen
	COMMAND-SHIFT-R	Wiederherstellen
	COMMAND-SHIFT-P	Wiederherstellen als
	COMMAND-SHIFT-A	Mit Administratorrechten arbeiten
Allgemein	COMMAND-,	Einstellungen
	COMMAND-SHIFT-S	Seitliche Infoleiste
	COMMAND-A	Alles markieren
	COMMAND-W	Schließen

Anhang D. Technischer Support

Den technischen Support von **Doctor Web** können Sie unter http://support.drweb.com/ kontaktieren.

Bei Problemen mit der Installation der Produkte nutzen Sie folgende Möglichkeiten, bevor Sie sich an den technischen Support wenden:

- Lesen Sie Produktinformationen und Anleitungen unter http://download.drweb.com/ durch
- Lesen Sie Häufig gestellte Fragen unter http://support.drweb.com/ durch
- Versuchen Sie, eine Antwort in der **Dr.Web Wissensdatenbank** unter http://wiki.drweb.com/ zu finden
- Besuchen Sie **Dr.Web Foren** unter http://forum.drweb.com/

Wenn Sie nicht geschafft haben, das Problem zu lösen, dann können Sie eine Web-Form einer Frage im Abschnitt unter http://support.drweb.com/ ausfüllen.

Die nächste Vertretung von **Doctor Web** und alle notwendigen Informationen über unser Unternehmen können Sie unter http://company.drweb.com/contacts/moscow finden.

Schlagwortregister

A

Abkürzungen 5
Administratorrechten 13, 21
Aktionen bei Bedrohungen 21
Antivirus-Prüfung 13
Antivirus-Reaktionen
  automatische 21
Anwendung
  Arten von Computerbedrohungen 24
  Beseitigung von Computerbedrohungen 31
  Tastenkombinationen 34
  technischer Support 35
Aufrufen der Hilfe 15
Ausnahme der Dateien 22
automatische Aktionen 21

B

Bearbeitung von Bedrohungen 16
Beenden der Arbeit 11
Beseitigung von Computerbedrohungen 31

C

Computerbedrohungen 24

D

Default-Parameter wiederherstellen 23
Deinstallation von Dr.Web Light 9
Dr.Web Hilfe 15
Dr.Web Light 7
  Aktualisierung 12
  Beenden der Arbeit 11
  Deinstallieren 9
  Einstellungen zurücksetzen 23
  Funktionen 7, 10, 16
  Hilfe 15
  Installieren 9
  Komponenten 7
  Prüfung nach Befehl 13
  Quarantäne 18
  Reaktionen 21
  Scan-Ergebnisse 16
  Starten 11
  Systemanforderungen 8
  technischer Support 35

E

Einstellungen 12, 21
  Administratorrechten 13
  Aktionen 21
  Ausnahmen 22
  Töne 21

Schlagwortregister

Einstellungen 12, 21
Zurücksetzen 23
Einstellungen zurücksetzenĸ 23

G

Grundfunktionen 10

H

hotkeys 34

I

Informationen zu Bedrohungen 16, 18
Installation von Dr.Web Light 9

M

Mein Dr.Web 10

P

Prüfung
Ausnahmen 22
benutzerdefiniert 13
schnell 13
vollständig 13
Prüfung im Akkubetrieb 21

Q

Quarantäne 18
Bearbeitung von Objekten 18
Informationen zu Bedrohungen 18

S

Scanner
automatische Aktionen 21
Starten vom Antivirus 11
Symbole 5
Systemanforderungen 8

T

Tastenkombinationen 34
technischer Support 35
Töne 21

U

Updater 12

Z

Zeitabstände 12

© 2009-2012 Doctor Web